The Dickson invariants and The Steenrod Algebra

A minor thesis submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
Mathematics PhD Degree Program

by
Jishu Das

under the supervision of

Dr. Steven Spallone

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road, Pashan, Pune India 411008

This is to certify that this minor thesis submitted towards the partial fulfillment of the Mathematics PhD degree program at the Indian Institute of Science Education and Research Pune, represents work carried out by Jishu Das under the supervision of Dr. Steven Spallone.

Dr. Steven Spallone
Minor Thesis Supervisor

Jishu Das
PhD Student

Acknowledgements

I would like to express my deep gratitude to Dr. Steven Spallone, my minor thesis supervisor, for his guidance, encouragement and useful critique of this minor thesis. I learnt a lot of things under his supervision. I would also like to thank Dr. Baskar Balasubramanyam and Dr. Kaneenika Sinha, my PhD thesis supervisors, for his/her encouragement to do such an interesting project. I would like to thank one of my senior Jyotirmoy Ganguly for many helpful discussions during the project. Last but not least, I would like to thank my friends for their support.

Contents

1 The Dickson Invariants

Let V be a finite dimensional vector space over the finite field $\mathbb{F}_q$. The ring of invariants of the full linear group $GL(V)$ was computed in early Twentieth Century by L.E. Dickson. The ring of invariants was found to be a graded polynomial algebra on certain generators called Dickson generators. This minor thesis is an attempt to understand these generator. In the next section we explore the Steenrod Algebra and try to see a connection of it with Dickson generators.

1.1 Introduction

Let $q = p^m$ where p is a prime number in $\mathbb{Z}$ and $m \in \mathbb{N}$. Let $\mathbb{F}_q$ be the finite field with q elements. The defining equation for $\mathbb{F}_q$ is given by

$$X^q = X$$

which is equivalent to

$$\prod_{a \in \mathbb{F}_q} (X - a) = 0$$

due to the fact that $\mathbb{F}_q$ is the splitting field of the separable polynomial

$$X^q - X \in \mathbb{F}_p[X]$$

whose roots are precisely the elements of $\mathbb{F}_q$.

Now let $n \in \mathbb{N}$ and V be a vector space of dimension n over $\mathbb{F}_q$. Further let us take R be the $\mathrm{Sym}(V)$. Using corollary 35 of section 11.5 from Dummit Foote [4], $\mathrm{Sym}(V)$ is isomorphic as a graded $\mathbb{F}_q$-algebra to the ring of polynomials in n variables over $\mathbb{F}_q$. Therefore R is a integral domain. Let K be the field of fraction of R, i.e. $K = \mathrm{Frac}(R)$. Consider the analogue defining equation for V.

$$f_n(X) = \prod_{v \in V} (X - v) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i} = 0$$

The second equality of the equation follows from equation 1.

Lemma 1.1. *Let*

$$f_n(X) = \prod_{v \in V} (X - v),$$

then there are $c_{n,i} \in K$ for $0 \leq i < n$, so that

$$f_n(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i}. \tag{1}$$

Proof. We have $f_n(X) = \prod_{v \in V}(X - v)$. Let $\{v_1, v_2, ..., v_n\}$ be a basis of V. Take V_i to be the subspace spanned by $\{v_1, v_2, ..., v_i\}$ for $i = 1, 2, ..., n-1$. For the vector space V, consider the following $(n+1) \times (n+1)$ matrix (say $D(X)$) given by

$$\begin{bmatrix} v_1 & v_2 & \dots & X \\ v_1^q & v_2^q & \dots & X^q \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ v_1^{q^n} & v_2^{q^n} & \dots & X^{q^n} \end{bmatrix}$$

Denote the determinant of the above matrix to be $\Delta_n(X)$.

Let $v = \sum_{i=1}^n \alpha_i v_i \in V$ where $\alpha_i \in \mathbb{F}_q$. Clearly $f_n(v) = 0$. In order to see what $\Delta_n(v)$ is, consider the column operation C_{n+1} replaced by $C_{n+1} - \sum_{i=1}^n \alpha_i C_i$ where C_i denotes i th column of the matrix $D(v)$. Observe for $k = 1, 2, .., n$ that

$$v^{q^k} = \big(\sum_{i=1}^n \alpha_i v_i\big)^{q^k} = \sum_{i=1}^n (\alpha_i v_i)^{q^k} = \sum_{i=1}^n \alpha_i v_i^{q^k}$$

since we are inside a field of characteristics p and $\alpha_i \in \mathbb{F}_q$. The above observation implies that after the column operation the entries in the last column of the matrix $D(v)$ is zero. Therefore $\Delta_n(v) = 0$.

Both $f_n(X)$ and $\Delta_n(X)$ are polynomial of degree q^n and can have at most q^n roots. Since $v \in V$, there are q^n distinct element in V which satisfy both $f_n(X)$ and $\Delta_n(X)$, $\Delta_n(X) = \lambda f_n(X)$ for some $\lambda \in K$. By expanding $\det(D(X))$ along last column we note that coefficient of X^{q^n} is $\Delta_{n-1}(v_n)$. This shows $\lambda = \Delta_{n-1}(v_n)$ as $f_n(X)$ is monic.

We show by induction on $n \in \mathbb{N} \cup \{0\}$ that $\Delta_{n-1}(v_n) \neq 0$ i.e. $\Delta_n(X)$ is a non zero polynomial. Let the assertion be true for vector space of dimension less than n, where we use V_i to define $\Delta_i(X)$ for $i = 1, 2, ..., n-1$ and set $\Delta_0(v_1) = v_1$. The first step of induction is trivial as $v_1 \neq 0$. By similar consideration as of V above, for V_{n-1} we can have

$$\Delta_{n-1}(v_n) = \Delta_{n-2}(v_{n-1}) f_{n-1}(v_n) \tag{2}$$

However $\Delta_{n-2}(v_{n-1}) \neq 0$ by induction hypothesis and

$$f_{n-1}(v_n) = \prod_{v \in V_{n-1}} (v_n - v) \neq 0$$

as $v_n \notin V_{n-1}$. Hence $\Delta_{n-1}(v_n) \neq 0$. Thus we have

$$f_n(X) = \frac{\Delta_n(X)}{\Delta_{n-1}(v_n)} = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i},$$

which is immediate by expanding $\det(D(X))$ along the last column.

□

For $n \in N$, $\{c_{n,i} \mid 0 \leq i \leq n-1\}$ are called Dickson generators.

Example 1.1. Let $q = 2$, $n = 2$ and $\{v_1, v_2\}$ be a basis of V. The Dickson generators are given by

$$c_{2,0} = v_1^2 v_2 + v_1 v_2^2, \;\; c_{2,1} = v_1^2 + v_2^2 + v_1 v_2.$$

Proof. Since $\{v_1, v_2\}$ be a basis of V, $V = \{0, v_1, v_2, v_1 + v_2\}$.

$$f_n(X) = \prod_{v \in V} (X - v) = X(X - v_1)(X - v_2)(X - (v_1 + v_2))$$

$$= X\big(X^2 - (v_1 + v_2)X + v_1 v_2\big)\big(X - (v_1 + v_2)\big)$$

$$= X\big(X^3 + [-(v_1 + v_2) - (v_1 + v_2)]X^2 + [(v_1 + v_2)^2 + v_1 v_2]X - [v_1 v_2 (v_1 + v_2)]\big)$$

$$= X\big(X^3 + (v_1^2 + v_2^2 + v_1 v_2)X - (v_1^2 v_2 + v_1 v_2^2)\big)$$

$$= X^4 + (v_1^2 + v_2^2 + v_1 v_2)X^2 - [v_1^2 v_2 + v_1 v_2^2]X$$

□

1.2 Recurrence relation for Dickson generators

Lemma 1.2. *If*

$$f_{n-1}(v_n) = \prod_{v \in V_{n-1}} (v_n - v)$$

as in Lemma 1.1, then

$$(i) \;\; f_{n-1}(X - a v_n) = f_{n-1}(X) - a f_{n-1}(v_n)$$

for a fixed $a \in \mathbb{F}_q$.
(ii)

$$\prod_{a \in \mathbb{F}_q} (f_{n-1}(X) - a f_{n-1}(v_n)) = f_{n-1}(X)^q - f_{n-1}(X)(f_{n-1}(v_n))^{q-1}.$$

Proof. Note that $\{w + a v_n \mid w \in V_{n-1}\}$ is the set of zeroes of $f_{n-1}(X - a v_n)$. Now for a fixed $w_0 \in V_{n-1}$ We have

$$f_{n-1}(w_0 + a v_n) - a f_{n-1}(v_n) = \prod_{w \in V_{n-1}} (w_0 + a v_n - w) - f_{n-1}(a v_n)$$

$$= \prod_{w \in V_{n-1}} (a v_n - (w - w_0)) - f_{n-1}(a v_n) = \prod_{\tilde{w} \in V_{n-1}} (a v_n - \tilde{w}) - f_{n-1}(a v_n)$$

$$= f_{n-1}(av_n) - f_{n-1}(av_n) = 0.$$

This shows $\{w+av_n \mid w \in V_{n-1}\}$ is also the set of zeroes of $f_{n-1}(X)-af_{n-1}(v_n)$. Both $f_{n-1}(X - av_n)$ and $f_{n-1}(X) - af_{n-1}(v_n)$ are monic have degree $q^{(n-1)^2}$, so $f_{n-1}(X - av_n) = f_{n-1}(X) - af_{n-1}(v_n)$ for a fixed $a \in \mathbb{F}_q$.

For (ii), consider the set $\{av_n \mid a \in \mathbb{F}_q\}$ which is the set of zeroes of $\prod_{a\in\mathbb{F}_q}(f_{n-1}(X) - af_{n-1}(v_n))$ as a polynomial in X.
For a fixed $a \in \mathbb{F}_q$,

$$\begin{aligned} &f_{n-1}(av_n)^q - f_{n-1}(av_n)(f_{n-1}(v_n))^{q-1} \\ &= a^q(f_{n-1}(v_n))^q - a(f_{n-1}(v_n))^q \\ &= a(f_{n-1}(v_n))^q - a(f_{n-1}(v_n))^q = 0. \end{aligned}$$

By similar argument as in (i), proof of (ii) is complete.

□

Theorem 1.3. *Let $B = \{v_1, v_2, ..., v_n\}$ be an ordered basis of V over $\mathbb{F}_q$.*
(i) Let A_B be the $(n+1) \times n$ matrix with entries $\{v_j^{q^i} : 0 \le i \le n, 1 \le j \le n\}$. If $A_B(i)$ is the matrix with the ith row deleted, then

$$c_{n,i} = \frac{\det(A_B(i))}{\Delta_{n-1}(v_n)}.$$

(ii) Let $V_{n-1} = span\{v_1, ..., v_{n-1}\}$, and $\{c_{n-1,i}\}$ be the Dickson generators for the invariants of $GL(V_{n-1})$. Then

$$c_{n,i} = c_{n-1,i-1}^q + c_{n-1,i}f_{n-1}(v_n)^{q-1}, \tag{3}$$

where

$$f_{n-1}(v_n) = \prod_{v\in V_{n-1}} (v_n - v).$$

Proof. By 2 We have

$$\Delta_n(X) = \Delta_{n-1}(v_n)f_n(X) = (\Delta_{n-1}(v_n))\Big(X^{q^n} + \sum_{i=0}^{n-1}(-1)^{n-i}c_{n,i}X^{q^i}\Big).$$

Expanding along $(n+1)$th column of $\Delta_n(X)$ and considering coefficient of X^{q^i}, it is clear that

$$c_{n,i} = \frac{\det(A_B(i))}{\Delta_{n-1}(v_n)}.$$

Note that every element $v \in V$ can be uniquely written as $av_n + w$ where $a \in \mathbb{F}_q$ and $w \in V_{n-1}$.

$$f_n(X) = \prod_{v\in V}(X - v) = \prod_{a\in\mathbb{F}_q}\Big(\prod_{w\in V_{n-1}}((X - av_n) - w)\Big)$$

$$= \prod_{a\in\mathbb{F}_q} f_{n-1}(X - av_n) = \prod_{a\in\mathbb{F}_q} (f_{n-1}(X) - af_{n-1}(v_n))$$

$$= f_{n-1}(X)^q - f_{n-1}(X)(f_{n-1}(v_n))^{q-1}.$$

By comparing coefficients on both sides we have,

$$c_{n,i} = c_{n-1,i-1}^q + c_{n-1,i} f_{n-1}(v_n)^{q-1}.$$

□

The $\mathbb{F}_q$ algebra generated by $\{c_{n,i} \mid 0 \le i \le n-1\}$ is called the Dickson algebra and $\{c_{n,i} \mid 0 \le i \le n-1\}$ are also called Dickson invariants.

Example 1.2. Let $q = 2$, $n = 3$ and $\{v_1, v_2, v_3\}$ be an ordered basis of V. Let

$$f_3(X) = X^8 - c_{3,2}X^4 + c_{3,1}X^2 - c_{3,0}X,$$

where $c_{3,2}, c_{3,1}$ and $c_{3,0}$ are given by

$$c_{3,2} = (v_1^2 + v_2^2 + v_1v_2)v_3^2 - (v_1^2v_2 + v_1v_2^2)v_3 + (v_1^4 + v_2^4 + v_1^4v_2^4),$$

$c_{3,1} = (v_1^2+v_2^2+v_1v_2)v_3^4+(v_1^4+v_2^4+(v_1v_2)^4)v_3^2-(v_1^4v_2+v_1v_2^4)v_3+(v_1^4v_2^2+v_1^2v_2^4)$,
and $c_{3,0} = \prod_{v\in V-\{0\}} v$.

Proof. Using equation 3 we have

$$c_{3,1} = c_{2,0}^2 + c_{2,1}f_2(v_3)$$

$= (v_1^2v_2 + v_1v_2^2)^2 + (v_1^2 + v_2^2 + v_1v_2)\big((v_3^4 + (v_1^2 + v_2^2 + v_1v_2)v_3^2 - (v_1^2v_2 + v_1v_2^2)v_3\big)$
$= v_1^4v_2^2+v_1^2v_2^4+(v_1^2+v_2^2+v_1v_2)v_3^4+(v_1^4+v_2^4+(v_1v_2)^4)v_3^2-(v_1^2+v_2^2+v_1v_2)(v_1^2v_2+v_1v_2^2)v_3$
$= (v_1^2 + v_2^2 + v_1v_2)v_3^4 + (v_1^4 + v_2^4 + (v_1v_2)^4)v_3^2 - (v_1^4v_2 + v_1v_2^4)v_3 + (v_1^4v_2^2 + v_1^2v_2^4)$
by using

$$(v_1^2 + v_2^2 + v_1v_2)(v_1^2v_2 + v_1v_2^2) = v_1^4v_2 + v_1^3v_2^2 + v_1^2v_2^3 + v_1v_2^4 + v_1^3v_2^2 + v_1^2v_2^3$$

$$= v_1^4v_2 + v_1v_2^4 + 2v_1^2v_2^3 + 2v_1^3v_2^2 = v_1^4v_2 + v_1v_2^4.$$

For

$$c_{3,2} = c_{2,1}^2 + c_{2,2}f_2(v_3)$$

$$= (v_1^2 + v_2^2 + v_1v_2)^2 + 1\big((v_1^2 + v_2^2 + v_1v_2)v_3^2 - (v_1^2v_2 + v_1v_2^2)v_3\big)$$

$$= (v_1^2 + v_2^2 + v_1v_2)v_3^2 - (v_1^2v_2 + v_1v_2^2)v_3 + (v_1^4 + v_2^4 + v_1^4v_2^4)$$

and

$$c_{3,0} = \prod_{v\in V-\{0\}} v.$$

□

Example 1.3. Let $q = 2$, $n \in \mathbb{N}$ and $\{v_1, v_2, ..., v_n\}$ be an ordered basis of V. Then for $1 \leq i \leq n-1$,

$$c_{n,i} = c_{n-1,i-1} + c_{n-1,i} f_{n-1}(v_n),$$

$$c_{n,0} = \prod_{v \in V - \{0\}} v.$$

Lemma 1.4. *Let $n \in \mathbb{N}$. The degree of $c_{n,i}$ is $q^n - q^i$ for $0 \leq i \leq n-1$ and $c_{n,i}$ is a homogeneous polynomial in $\{v_1, ..., v_n\}$.*

Proof. Let $n \in \mathbb{N}$ be fixed. It is clear from example 1.3 that the degree of $c_{n,0}$ is $q^n - 1$. Since

$$\prod_{v \in V} (X - v) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i},$$

we have

$$c_{n,i} = \sum_{1 \leq j_1 < ... < j_{q^n - q^i} \leq q^n} w_{j_1} ... \, w_{j_k}$$

where $w_{j_l} \in V$.

This shows that degree of $c_{n,i}$ is $q^n - q^i$ as we can take $w_{j_1}, ..., w_{j_{q^n - q^i}}$ such that $w_l \neq 0$ for $1 \leq l \leq q^n - q^i$. Since c_{n_i} is sum of terms of equal degree in $\{v_1, ..., v_n\}$, it is a homogeneous polynomial in $\{v_1, ..., v_n\}$.

□

1.3 Main Theorem

The group $GL_n(\mathbb{F}_q)$ acts on $\mathbb{F}_q[v_1, ..., v_n]$ by linear transformation i.e.
For $g \in GL_n(\mathbb{F}_q)$, $g = (g_{ij})$ and $f \in \mathbb{F}_q[v_1, ..., v_n]$, set $f^g = f(v'_1, ..., v'_n)$ where $v_i = \sum_{j=1}^{n} g_{ij} v_j$.

The ring of $GL_n(\mathbb{F}_q)$ invariants is defined to be
$\{ f \in \mathbb{F}_q[v_1, ..., v_n] \mid f^g = f \text{ for all } g \in GL_n(\mathbb{F}_q) \}$. We denote the ring of invariants as $\mathbb{F}_q[v_1, ..., v_n])^{GL_n(V)}$. Now we try to see how the ring of invariant is related with Dickson generators. The proof of Lemma 1.5 and Theorem 1.6 is followed from Cohomology of finite groups [3].

Let $\{v_1, ..., v_n\}$ be an ordered basis of V. Let $\mathcal{A}_n$ be the ring spanned by $\{c_{n,0}, c_{n,1}, ... , c_{n,n-1}\}$. Note that $\mathbb{F}_q[v_1, ..., v_n]$ is integral over $\mathcal{A}_n$ as each v_j are integral over $\mathcal{A}_n$. This is because

$$f_n(v_j) = \prod_{v \in V} (v_j - v) = 0 = (v_j)^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} \big(v_j\big)^{q^i}.$$

Lemma 1.5. *Frac($\mathbb{F}_q[v_1, ..., v_n]$) is Galois over Frac($\mathcal{A}_n$) and the Galois group is given by $GL_n(\mathbb{F}_q)$.*

Proof. In first step we show $\mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n])$ is the splitting field of $f_n(X)$ over the field $\mathrm{Frac}(\mathcal{A}_n)$. Let K' be the splitting field of $f_n(X)$ over the field $\mathrm{Frac}(\mathcal{A}_n)$. The polynomial $f_n(X)$ factors completely in $\mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n])$, so by definition of splitting field $K' \subset \mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n])$. Since $v_1, ..., v_n$ are roots of $f_n(X)$, $v_1, ..., v_n \in K'$. So have $\mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n]) \subset K'$. Moreover the polynomial $f_n(X)$ has no repeated roots which implies the extension is separable and therefore Galois.

Let G be the Galois group of K' over $\mathrm{Frac}(\mathcal{A}_n)$. Now for $g \in G$ and $\alpha_i \in \mathbb{F}_q$, we have

$$g\big(\sum_1^n \alpha_i v_i\big) = \sum_1^n \alpha_i g(v_i).$$

This is because $\mathbb{F}_q \subset \mathcal{A}_n$, g fixes $\mathrm{Frac}(\mathcal{A}_n)$ and g acts to permute the roots of $f_n(X)$. Hence $g(v_i) = \sum_{i=1}^n g_{ij} v_j$. So $g \in GL_n(\mathbb{F}_q)$.

Conversely let $g \in GL_n(\mathbb{F}_q)$. We have

$$c_{n,i} = \sum_{1 \le j_1 < ... < j_{q^n - q^i} \le q^n} w_{j_1} ... \, w_{j_k}$$

where $w_{j_l} \in V$. Since g maps V onto V we see that g fixes $c_{n,i}$. This implies that g fixes $\mathrm{Frac}(\mathcal{A}_n)$. Now g acts as an automorphism in K' by construction. So $g \in G$. □

We use the Lemma to show that the ring of invariants of $\mathbb{F}_q[v_1, ..., v_n])^{GL_n(V)}$ is $\mathbb{F}_q[c_{n,0}, c_{n,1}, ... \, , c_{n,n-1}]$.

Theorem 1.6. *The ring of invariants of $\mathbb{F}_q[v_1, ..., v_n])^{GL_n(V)}$ is*

$$\mathbb{F}_q[c_{n,0}, c_{n,1}, ... \, , c_{n,n-1}].$$

Proof. $\mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n])$ is finitely generated over $\mathrm{Frac}(\mathcal{A}_n)$. Hence $\mathbb{F}_q[v_1, ..., v_n]$ is finitely generated extension of integral closure of $\mathcal{A}_n$ in $\mathrm{Frac}(\mathcal{A}_n)$. This implies $\mathbb{F}_q[v_1, ..., v_n]$ and integral closure of $\mathcal{A}_n$ both have same transcendence degree. $\mathbb{F}_q[v_1, ..., v_n]$ has transcendence degree n and $\mathcal{A}_n$ is generated by n elements over $\mathbb{F}_q$, so $\{c_{n,0}, c_{n,1}, ... \, , c_{n,n-1}\}$ are algebraically independent. Therefore $\mathcal{A}_n = \mathbb{F}_q[c_{n,0}, c_{n,1}, ... \, , c_{n,n-1}]$. (Please refer to example 19.19 of chapter V of Morandi [5].)

$\mathbb{F}_q[v_1, ..., v_n]$ is integrally closed in $\mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n])$ as a UFD is integrally closed (See examples below corollary 25 of section 15.3 in Dummit Foote [4]). We have $\mathbb{F}_q[v_1, ..., v_n] \cap \mathrm{Frac}(\mathcal{A}_n)$ to be the ring of $GL_n(\mathbb{F}_q)$ invariants in $\mathbb{F}_q[v_1, ..., v_n]$ since the fixed field of $GL_n(\mathbb{F}_q)$ for the Galois extension $\mathrm{Frac}(\mathbb{F}_q[v_1, ..., v_n])$ over $\mathrm{Frac}(\mathcal{A}_n)$ is $\mathrm{Frac}(\mathcal{A}_n)$.

Now $\mathbb{F}_q[v_1, ..., v_n] \cap \text{Frac}(\mathcal{A}_n)$ is integral over $\mathcal{A}_n$ in its quotient field as $\mathbb{F}_q[v_1, ..., v_n]$ is integral over $\mathcal{A}_n$. However $\mathcal{A}_n = \mathbb{F}_q[c_{n,0}, c_{n,1}, \dots, c_{n,n-1}]$ is integrally closed. Therefore $\mathbb{F}_q[v_1, ..., v_n] \cap \text{Frac}(\mathcal{A}_n) = \mathcal{A}_n = \mathbb{F}_q[c_{n,0}, c_{n,1}, \dots, c_{n,n-1}]$. $\square$

2 The Steenrod Algebra

2.1 Introduction

Let $\mathbb{F}_q[V]$ denote the symmetric algebra on the dual vector space V^* of V. Note that

$$\mathbb{F}_q[V] = \bigoplus_{k=0}^{\infty} S^k(V^*)$$

where $S^k(V^*)$ is the kth symmetric power of V^*. Let $\mathbb{F}_q[V][[\xi]]$ denote the power series ring over $\mathbb{F}_q[V]$ in an additional variable ξ. Consider the map $\tilde{\mathcal{P}}(\xi)(l) = l + l^q\xi \in \mathbb{F}_q[V][[\xi]]$ where $l^r = l \otimes ...r$ times $\otimes\, l$ for $l \in V^*$. Note that

$$\tilde{\mathcal{P}}(\xi)(l_1 + l_2) = (l_1 + l_2) + (l_1 + l_2)^q\xi = l_1 + l_2 + (l_1^q + l_2^q)\xi = \tilde{\mathcal{P}}(\xi)(l_1) + \tilde{\mathcal{P}}(\xi)(l_2)$$

for $l_1, l_2 \in V^*$ and also

$$\tilde{\mathcal{P}}(\xi)(\alpha l) = \alpha l + (\alpha l)^q\xi = \alpha l + \alpha^q l^q\xi = \alpha l + \alpha l^q\xi = \alpha\tilde{\mathcal{P}}(\xi)(l)$$

for $l \in V^*$ and $\alpha \in \mathbb{F}_q$. By universal property of symmetric algebra (see Theorem 34 (3) from section 11.5 of Dummit Foote [4]) there exists an unique $\mathbb{F}_{\shortparallel}$ algebra homomorphism $\mathcal{P}(\xi) : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V][[\xi]]$ such that $\mathcal{P}(\xi)$ restricted to V^* is equal to $\tilde{\mathcal{P}}$.

Let $k \in \mathbb{N} \cup \{0\}$ and define $\mathcal{P}^k : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V]$ by $\mathcal{P}^k(f) = Pr_k(\mathcal{P}(\xi)(f))$ where $Pr_k : \mathbb{F}_q[V][[\xi]] \longrightarrow \mathbb{F}_q[V]$ is given by

$$Pr_k\Big(\sum_{i=0}^{\infty} a_i\xi^i\Big) = a_k$$

The map $\mathcal{P}^k$ is a $\mathbb{F}_q$ linear map since it is a composition of two $\mathbb{F}_q$ linear maps.

Let $f \in \mathbb{F}_q[V]$ then we can always write $f = f_0 + ... + f_t$ for some $t \in \mathbb{N} \cup \{0\}$ and $f_i \in S^k(V^*)$ for $i = 0, 1, .., t$.
We let $\deg(f) = \min\{t \in \mathbb{N} \cup \{0\} \mid f_t \neq 0 \text{ for } f \neq 0\}$.

Lemma 2.1. *If $f \in \mathbb{F}_q[V]$ and $f = f_0 + ... + f_t$ where $t = deg(f)$, then*

$$\mathcal{P}^i(f) = \begin{cases} f_t^q & \text{if } i = t \\ 0 & \text{if } i > t \end{cases}.$$

(4)

Proof. Let $f_i = l_{1i} \otimes ... \otimes l_{ii}$ for $i \in \mathbb{N}$, then

$$\mathcal{P}(\xi)(f) = \sum_{i=0}^{t} \mathcal{P}(\xi)(f_i) = f_0 + \sum_{i=1}^{t} \mathcal{P}(\xi)(l_{1i} \otimes ... \otimes l_{ii})$$

$$= f_0 + \sum_{i=1}^{t} \mathcal{P}(\xi)(l_{1i}) \otimes ... \otimes \mathcal{P}(\xi)(l_{ii}) = f_0 + \sum_{i=1}^{t} (l_{1i} + l_{1i}^q \xi) \otimes ... \otimes (l_{ii} + l_{ii}^q \xi)$$

$$= f_0 + \Big(\sum_{i=1}^{t-1} (l_{1i} + l_{1i}^q \xi) \otimes ... \otimes (l_{ii} + l_{ii}^q \xi) \Big) + \big((l_{1t} + l_{1t}^q \xi) \otimes ... \otimes (l_{tt} + l_{tt}^q \xi) \big).$$

The highest power of ξ in $\mathcal{P}(\xi)(f)$ is t and the coefficient to ξ^t is given by $l_{1t}^q \otimes ... \otimes l_{tt}^q = \big(l_{1t} \otimes ... \otimes l_{tt}\big)^q$. Note that

$$\mathcal{P}^t(f) = \mathcal{P}^t(f_0) + \sum_{i=1}^{t} \mathcal{P}^t(f_i) = \mathcal{P}^t(f_0) + \mathcal{P}^t(f_t)$$

since $\deg(f_i) = i$ and $\mathcal{P}^k(f_i) = 0$ for $1 \leq i < t$. However

$$\mathcal{P}^t(f_t) = \mathcal{P}^t(l_{1t} \otimes ... \otimes l_{tt}) = (l_{1t} \otimes ... \otimes l_{tt})^q$$

. Thus $\mathcal{P}^t(f_0) = 0$ and we have

$$\mathcal{P}^t(f) = \mathcal{P}^t(f_t) = (l_{1t} \otimes ... \otimes l_{tt})^q = f_t^q.$$

□

In particular for $l \in V^*$, $\mathcal{P}^0(v) = v$, $\mathcal{P}^1(v) = v^q$ and $\mathcal{P}^k(v) = 0$ for $k > 1$.

2.2 Cartan's formulae

Lemma 2.2. *$\mathcal{P}^k(fg) = \sum_{i+j=k} \mathcal{P}^i(f)\, \mathcal{P}^j(g)$ for $k \in \mathbb{N}$ and $f, g \in \mathbb{F}_q[V]$.*

Proof. Let $k \in \mathbb{N}$. Consider

$$Pr_k\Big((\sum_{i=0}^{\infty} a_i \xi^i)(\sum_{j=0}^{\infty} b_i \xi^j) \Big) = Pr_k\Big(\sum_{l=0}^{\infty} (\sum_{i=0}^{l} a_i b_{l-i}) \xi^l \Big)$$

$$\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} Pr_i\Big(\sum_{i=0}^{\infty} a_i \xi^i \Big) Pr_{k-i}\Big(\sum_{j=0}^{\infty} a_i \xi^j \Big).$$

This proves the lemma. □

These are called the *Cartan formulae* for the Steenrod operations.

Lemma 2.3.

$$\mathcal{P}^k(f_1\ f_2\ ...\ f_r) = \sum_{i_1+...+i_r=k} \mathcal{P}^{i_1}(f_1)\ \mathcal{P}^{i_2}(f_2)\ ...\ \mathcal{P}^{i_l}(f_r)$$

for $k, r \in \mathbb{N}$ *and* $f_i \in \mathbb{F}_q[V]$ *for* $i = 1, 2, ..., r$.

Proof. We use induction on r. For $r = 1$ the lemma is true. Let the assertion be true for r. Now using Cartan formulae with $f = f_1\ f_2\ ...\ f_r$ and $g = f_{r+1}$,

$$\mathcal{P}^k(f_1\ f_2\ ...\ f_{r+1}) = \sum_{i+j=k} \mathcal{P}^i(f_1\ f_2\ ...\ f_r)\mathcal{P}^j(f_{r+1})$$

$$= \sum_{i+j=k} \Big(\sum_{i_1+...+i_l=i} \mathcal{P}^{i_1}(f_1)\ \mathcal{P}^{i_2}(f_2)\ ...\ \mathcal{P}^{i_r}(f_r)\ \Big)\mathcal{P}^j(f_{r+1})$$

$$= \sum_{i+j=k} \Big(\sum_{i_1+...+i_l=i} \mathcal{P}^{i_1}(f_1)\ \mathcal{P}^{i_2}(f_2)\ ...\ \mathcal{P}^{i_r}(f_r)\ \mathcal{P}^j(f_{r+1})\Big)$$

$$= \sum_{i_1+...+i_{r+1}=k} \mathcal{P}^{i_1}(f_1)\ \mathcal{P}^{i_2}(f_2)\ ...\ \mathcal{P}^{i_{r+1}}(f_{r+1})$$

by taking $j = i_{r+1}$.

□

Let us consider one simple example by using Cartan's formula for $q = 2$.

Example 2.1. Let$\{l_1, l_2\}$ be an ordered basis of V^*. If $f = l_1^2 + l_1 \otimes l_2 + l_2^2 \in \mathbb{F}_2[V]$, then

$$\mathcal{P}^k(f) = \begin{cases} l_1^2 \otimes l_2 + l_1 \otimes l_2^2 & \text{if k = 1,} \\ l_1^4 + l_1^2 \otimes l_2^2 + l_2^4 & \text{if k = 2,} \\ 0 & \text{if } k > 2. \end{cases}$$

Proof. We start with $k = 1$.

$$\mathcal{P}^1(l_1^2) = \mathcal{P}^1(l_1 \otimes l_1) = \mathcal{P}^0(l_1)\mathcal{P}^1(l_1) + \mathcal{P}^1(l_1)\mathcal{P}^0(l_1)$$

$$= l_1 \otimes l_1^2 + l_1^2 \otimes l_1 = l_1^3 + l_1^3 = 0.$$

Similarly we have $\mathcal{P}^1(l_2^2) = 0$

$$\mathcal{P}^1(l_1 \otimes l_2) = \mathcal{P}^1(l_1)\mathcal{P}^0(l_2) + \mathcal{P}^0(l_1)\mathcal{P}^1(l_2)$$

$$= l_1^2 \otimes l_2 + l_1 \otimes l_2^2.$$

Now we proceed for $k = 2$.

$$\mathcal{P}^2(l_1^2 + l_1 \otimes l_2 + l_2^2) = \mathcal{P}^2(l_1^2) + \mathcal{P}^2(l_1 \otimes l_2) + \mathcal{P}^2(l_2^2)$$

$$= (l_1^2)^2 + (l_1 \otimes l_2)^2 + (l_2^2)^2 = l_1^4 + l_1^2 \otimes l_2^2 + l_2^4$$

by Lemma 2.1
The case for $k > 2$ follows easily again from Lemma 2.1. □

Let V and V' be two finite dimensional vector spaces over $\mathbb{F}_q$ and $T: V \to V'$ be a $\mathbb{F}_q$ linear map. The map T induces the map $T^* : (V')^* \to V^*$ which is given by $T^*(l) = l \circ T$. The map T^* further induces a map $\mathrm{Sym}(T^*) : \mathbb{F}_q[V'] \to \mathbb{F}_q[V]$ which sends a simple t tensor $l'_1 \otimes ... \otimes l'_t$ to $T^*(l'_1) \otimes ... \otimes T^*(l'_t)$. It is not difficult to show that $\mathrm{Sym}(T^*)$ is a $\mathbb{F}_q$ algebra homomorphism. The map $\mathrm{Sym}(T^*)$ induces another $\mathbb{F}_q$ algebra homomorphism $\mathrm{Sym}(T^*)(\xi)$ from $\mathbb{F}_q[V'][[\xi]]$ to $\mathbb{F}_q[V][[\xi]]$ by sending $(l'_1 \otimes ... \otimes l'_t)\xi^r$ to $(T^*(l'_1) \otimes ... \otimes T^*(l'_t))\xi^r$ for a simple t tensor and $r \in \mathbb{N}$. We have the following lemma.

Lemma 2.4. *Let V and V' be two finite dimensional vector spaces over $\mathbb{F}_q$ and $T: V \to V'$ be a $\mathbb{F}_q$ linear map. Let $\mathcal{P}(\xi)$ and $\mathcal{P}'(\xi)$ be the maps defined earlier for V and V' respectively. Then $\mathcal{P}(\xi) \circ \mathrm{Sym}(T^*) = \mathrm{Sym}(T^*)(\xi) \circ \mathcal{P}'(\xi)$.*

Proof. All the maps involved are $\mathbb{F}_q$ linear maps, hence it is enough to show that the maps agree for a simple t tensor $l'_1 \otimes ... \otimes l'_t$. If we let $T^*(l'_i) = l_i$ for $i = 1, 2, ..., t$, then for the left hand side we have

$$\mathcal{P}(\xi)(\mathrm{Sym}(T^*))(l'_1 \otimes ... \otimes l'_t) = \mathcal{P}(\xi)(l_1 \otimes ... \otimes l_t)$$

but $\mathcal{P}(\xi)$ is a $\mathbb{F}_{||}$ algebra homomorphism so

$$\mathcal{P}(\xi)(l_1 \otimes ... \otimes l_t) = (l_1 + l_1^q\xi) \otimes ... \otimes (l_t + l_t^q\xi)$$

For the right hand side

$$\mathrm{Sym}(T^*)(\xi)(\mathcal{P}'(\xi)(l'_1 \otimes ... \otimes l'_t)) = \mathrm{Sym}(T^*)(\xi)((l'_1 + {l'_1}^q\xi) \otimes ... \otimes (l'_t + {l'_t}^q\xi))$$

As $\mathrm{Sym}(T^*)(\xi)$ is a $\mathbb{F}_{||}$ algebra homomorphism

$$\begin{aligned}
&\mathrm{Sym}(T^*)(\xi)((l'_1 + {l'_1}^q\xi) \otimes ... \otimes (l'_t + {l'_t}^q\xi)) \\
&= \big(\mathrm{Sym}(T^*)(\xi)(l'_1 + {l'_1}^q\xi)\big) \otimes ... \otimes \big(\mathrm{Sym}(T^*)(\xi)(l'_t + {l'_t}^q\xi\big) \\
&= \big((T^*(l'_1) + T^*(l'_1)^q)\xi\big) \otimes ... \otimes \big((T^*(l'_t) + T^*(l'_t)^q)\xi\big) \\
&= (l_1 + l_1^q\xi) \otimes ... \otimes (l_t + l_t^q\xi)
\end{aligned}$$

Therefore we have the following commutative diagram.

$$\begin{array}{ccc}
\mathbb{F}_q[V'] & \xrightarrow{\mathrm{Sym}(T^*)} & \mathbb{F}_q[V] \\
\big\downarrow \mathcal{P}'(\xi) & & \big\downarrow \mathcal{P}(\xi) \\
\mathbb{F}_q[V'][[\xi]] & \xrightarrow{\mathrm{Sym}(T^*)(\xi)} & \mathbb{F}_q[V][[\xi]]
\end{array}$$

□

Note that $V*$ and V are finite dimensional and are isomorphic as $\mathbb{F}_q$ vector space. By virtue of Lemma 2.4 we can consider $\mathcal{P}^k$ acting on Dickson generators.

2.3 The Steenrod Algebra action

Now we restrict our focus to the case $q = p$.

Proposition 2.1. For

$$f(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i},$$

$f(X)$ divides $\mathcal{P}^k(f(X))$ in $\mathbb{F}_q[c_{n,0}, ...c_{n,n-1}][X]$.
Furthermore

$$\mathcal{P}^k(f(X)) = -f(X)(\mathcal{P}^{k-p^{n-1}}(c_{n,n-i}))$$

for $k \neq p^n, 0$.
$\mathcal{P}^{p^n}(f(X)) = (f(X))^p$, where $\mathcal{P}^j \equiv 0$ for $j < 0$, $c_{n,n} = 1$ and $c_{n,j} = 0$ for $j < 0$.

Proof. Let $I = \{i_1, ...i_k\}$ be an index set such that $v_t \in V$ for $t \in I$. We have

$$\mathcal{P}^k(f(X)) = \mathcal{P}^k\Big(\prod_{v \in V}(X - v)\Big)$$

$$= \sum_I \mathcal{P}^1(X - v_{i_1})...\mathcal{P}^1(X - v_{i_k})\Big(\prod_{v - \{i_1,...i_k\}} \mathcal{P}^0(X - v)\Big)$$

$$= \sum_I (X - v_{i_1})^p ...(X - v_{i_k})^p \Big(\prod_{v - \{i_1,...i_k\}} (X - v)\Big)$$

$$= \Big(\prod_{v \in V}(X - v)\Big) \sum_I (X - v_{i_1})^{p-1} ...(X - v_{i_k})^{p-1}$$

$$= f(X) \sum_I (X - v_{i_1})^{p-1} ...(X - v_{i_k})^{p-1}.$$

Hence $f(X)$ divides $\mathcal{P}^k(f(X))$ in $\mathbb{F}_q[c_{n,0}, ...c_{n,n-1}[X]$.

If x_2 is 2 dimensional (one dimesional for $p = 2$), then for $j \neq p^i$ and 0,

$$\mathcal{P}^j(x_2^{p^i}) = \sum_{i_1 + ... i_{p^i} = j} \frac{(p^i + j - 1)!}{(p^i - 1)! j!} \prod_{t \in \{i_1, ...i_k\}} \mathcal{P}^t(x_2),$$

since the number of non-negative integral solutions of equation $i_1 + ... + i_n = r$ is given by $\frac{(n+r-1)!}{(n-1)!r!}$. Since p divides $\frac{(p^i+j-1)!}{(p^i-1)!j!}$ we have $\mathcal{P}^j(x_2^{p^i}) = 0$.
We also have $\mathcal{P}^{p^i}(x_2^{p^i}) = x_2^{p^{i+1}}$. Using these results in

$$f(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{q^i}$$

and rearranging we have

$$\mathcal{P}^k(f(X)) = \sum_{i=0}^{n-1}(-1)^{n-i}(\mathcal{P}^{k-p^i}c_n, i)X^{p^{i+1}} + \sum_{i=0}^{n-1}(-1)^{n-i}(\mathcal{P}^k c_n, i)X^{p^i}$$

for $k \neq p^n, 0$. This has degree at most p^n in X. However $f(X)$ divides $\mathcal{P}^k(f(X))$ implies degree of $\mathcal{P}^k(f(X))$ is at least p^n. This shows degree of $\mathcal{P}^k(f(X))$is p^n. On equating the leading coefficient we have

$$\mathcal{P}^k(f(x)) = -f(X)(\mathcal{P}^{k-p^{n-1}}(c_{n,n-i})).$$

The case $k = p^n$ follows from Lemma 2.1. □

Remark. The Steenrod operations restricted to the ring of invariants $\mathbb{F}_q[v_1, ..., v_n])^{GL_n(V)}$ map Dickson invariants to Dickson invariants. Hence they can be used to produce new invariants from the old ones. More on this remark can be found at Larry Smith [1].

References

[1] Larry Smith, *An algebraic introduction to the Steenrod algebra*. Geometry and Topology Monographs, 11(207), 327-348.

[2] Clarence Wilkerson, *A primer on the Dickson invariants*, Purdue University.

[3] Alejandro Adem and R. James Milgram, *Cohomology of Finite Groups*, Springer - Verlag.

[4] David S. Dummit and Richard M. Foote, *Abstract Algebra*, Third Edition, John Wiley Sons, Inc.

[5] Patrick Morandi, *Field and Galois Theory*, 1996, Springer-Verlag, New York, Inc.